보안공부닷컴
http://www.boangongbu.com

개나소나 다하는 해킹 – 원격제어
(ProRat)

작성날짜: 2010년 5월 19일 수요일

메일주소: boangongbu@naver.com

Sub7 강좌를 먼저 작성하고 싶었지만 공식사이트 http://www.subseven.org 에 접속해보니 조만간에 새로운 버전 2.3.1 이 선보이게 된다고 하네요. 10년 만의 부활이라 기대됨.

그럼 일단 비슷한 프로그램인 ProRat 사용법을 소개해 드리도록 하겠습니다. 터키 개발자가 개발하게 되었고 공식사이트는 http://www.prorat.net . 파일은 공식사이트에서 받도록 하세요.

여러가지 언어파일을 제공하고 있지만 아직 한글은 없네요. (현재 보안공부닷컴에서 한글화중이지만 언제 완료될지는 ... ^^)

일단 다운받고 메인창을 열어보면

네.... 넷데빌하고 비슷하죠?

아래에 계속하여 하나하나 알아보도록 하죠.

(0) **스킨매니저**: 클릭하시면 스킨선택창이 뜹니다.

(1) **언인스톨**: 클릭하시면 서버프로그램 삭제 창이 뜹니다.

(2) **다운로드폴더**: ProRat를 사용하여 파일다운로드시 파일이 저정된 폴더로 이동됩니다.

(3) **온라인뉴스**: ProRat 공식사이트 공지사항이 뜹니다.

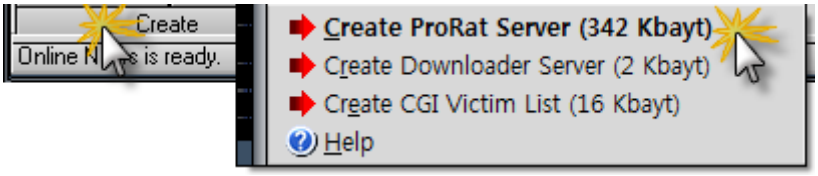
(4) **정보**: ProRat 실행시 메인창으로 이동.

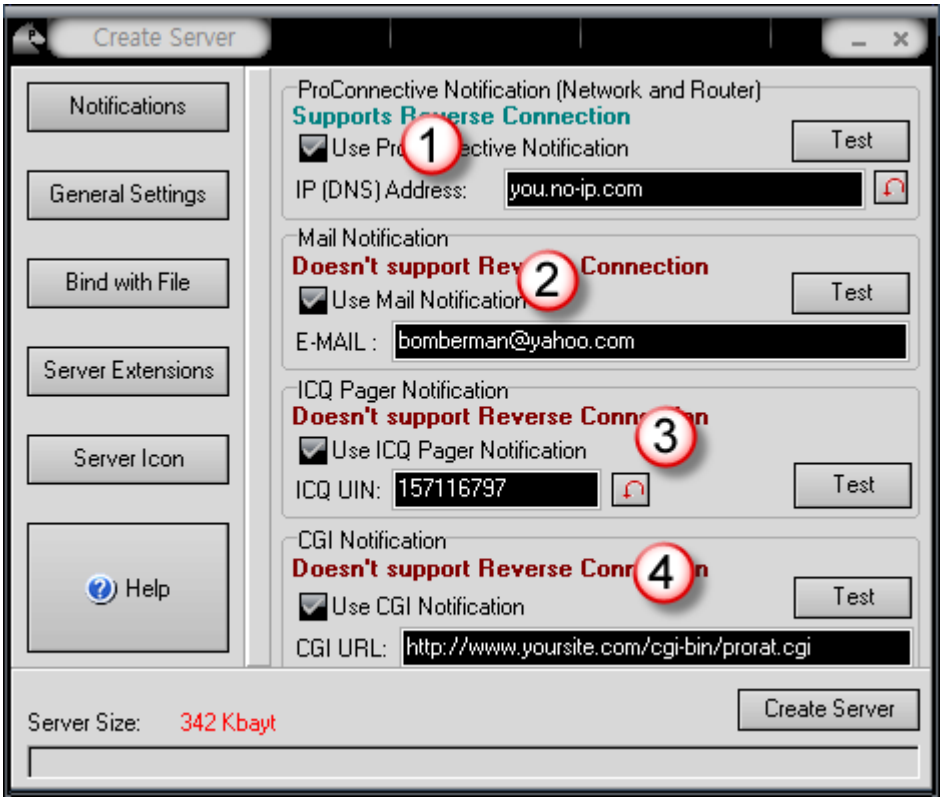
(5) **도움말**: 도움말파일 실행.

(6) **구매정보**: 구매를 원할시 클릭하시면 상세한 구매방법이 뜹니다.

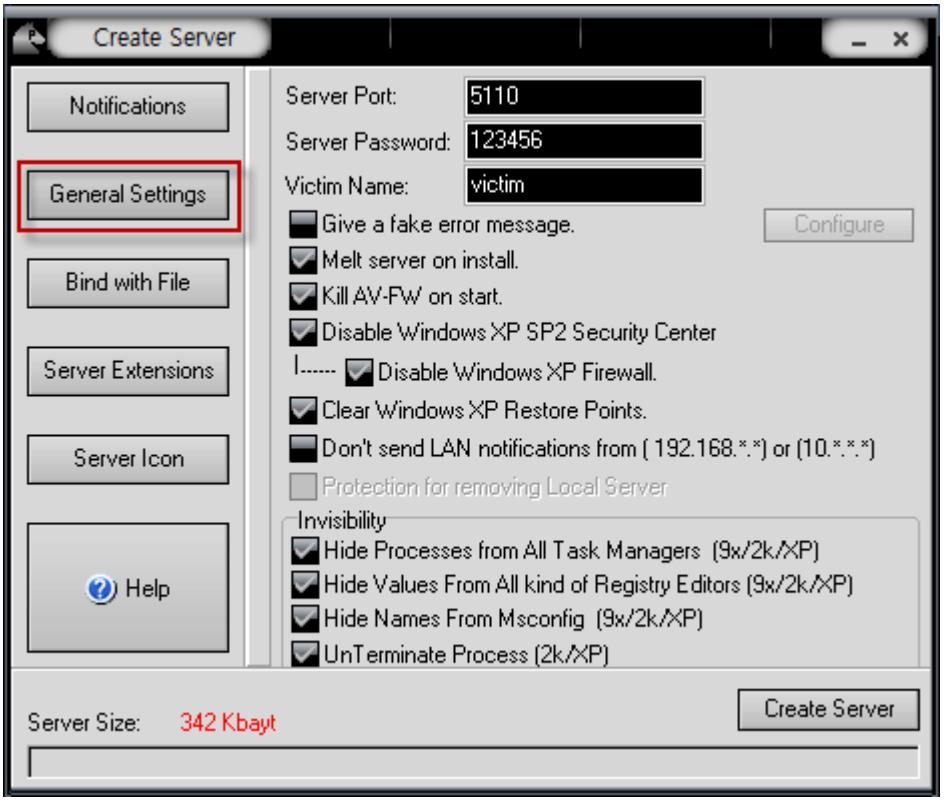
역시 제일처음 해야될 것은 서버파일 만드는거죠?

아래그림대로 왼쪽메뉴 맨아래 "Create"(제작)을 클릭하시고 "Create ProRat Server 를 클릭하시면 서버파일생성창이 뜰것이구요.





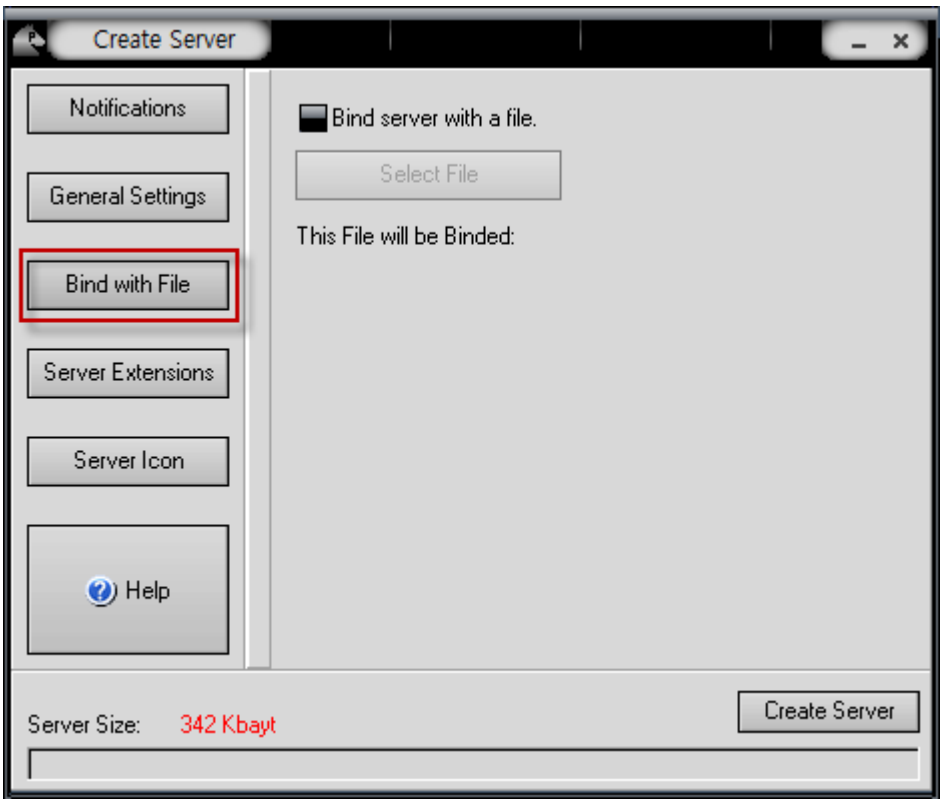
위와 같은 창이 뜨는데 여기선 좀비PC의 접속정보 획득방법을 설택하고 설정하는 곳인데요 (1)번은 리버스컨넥션을 지원하는 접속법, (2)번은 메일로 정보를 보내주는 방법. (3)번은 ICQ로 정보를 보내주는 방법. (4)번은 웹사이트에서 정보를 확인하는 방법으로 나뉘는데요. 넷데빌보다 많아진 옵션은 (1)번 리버스컨넥션이 겠습니다. 말 그대로 거꾸로 접속하는 방법. 좀비PC의 아이피가 바뀐다 하여도 설정된 아이피 혹은 도메인으로 접속을 시도하는것이죠. 만약 도메인을 설정하셨다면 아이피에 상관없이 좀비PC에 대한 모니터링이 가능하겠죠? (예를 들면 http://www.codns.com 같은 서비스를 사용한다면)



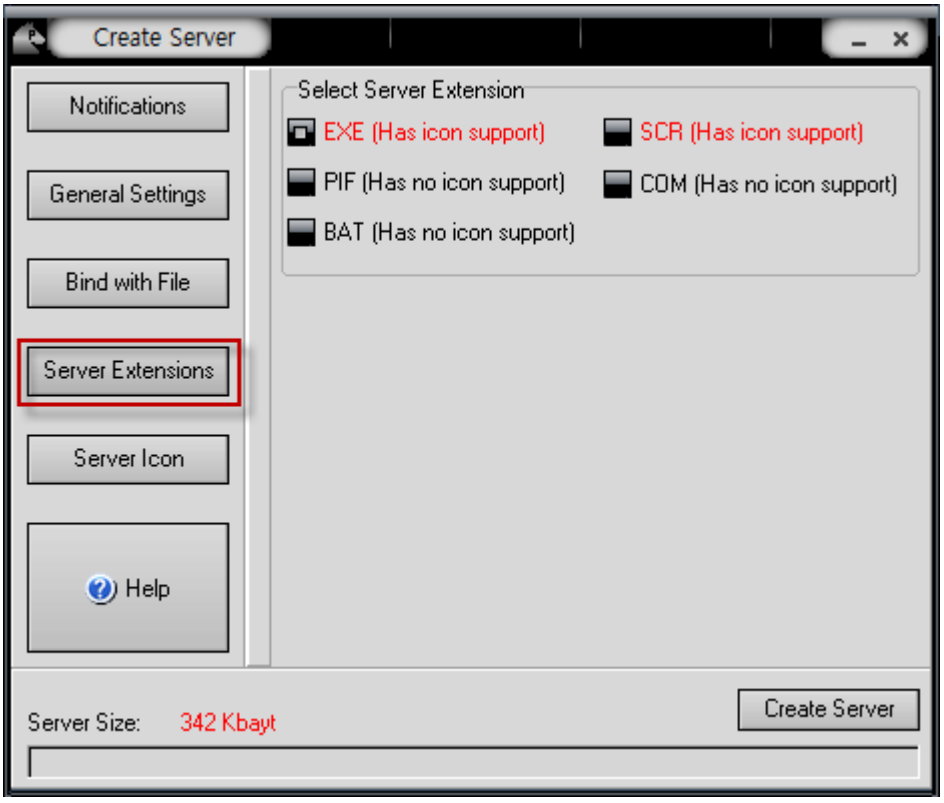
두번째 설정페이지. 서버포트(클라이언트에서 접속시 사용되는 포트). 서버 패스워드(클라이언트에서 접속시 입력해야될 패스워드.). 좀비PC 이름. "Give a fake error message" (서버파일을 실행하였을 때 에러창 띄우기). "Melt server on install"(서버파일을 실행하고 자신을 삭제). "Kill AV-FW on start" (방화벽하고 백신프로그램을 정지하기). "Disable Windows XP SP2 Security Center"(윈도우xp 보안센트와 방화벽기능을 정지하기). "Clear Windows XP Restore Points"(윈도우xp복구점 삭제하기). "Don't send LAN notifications from..."(내부망컴퓨터에서 정보를 보내지 않는다고 씌여져 있는데 뭔 기능인지 감이 안잡힘. 그리고 proconnective 접속을 사용하여야 되구요. 유료사용

자만 지원되는 기능이라고 하네요)

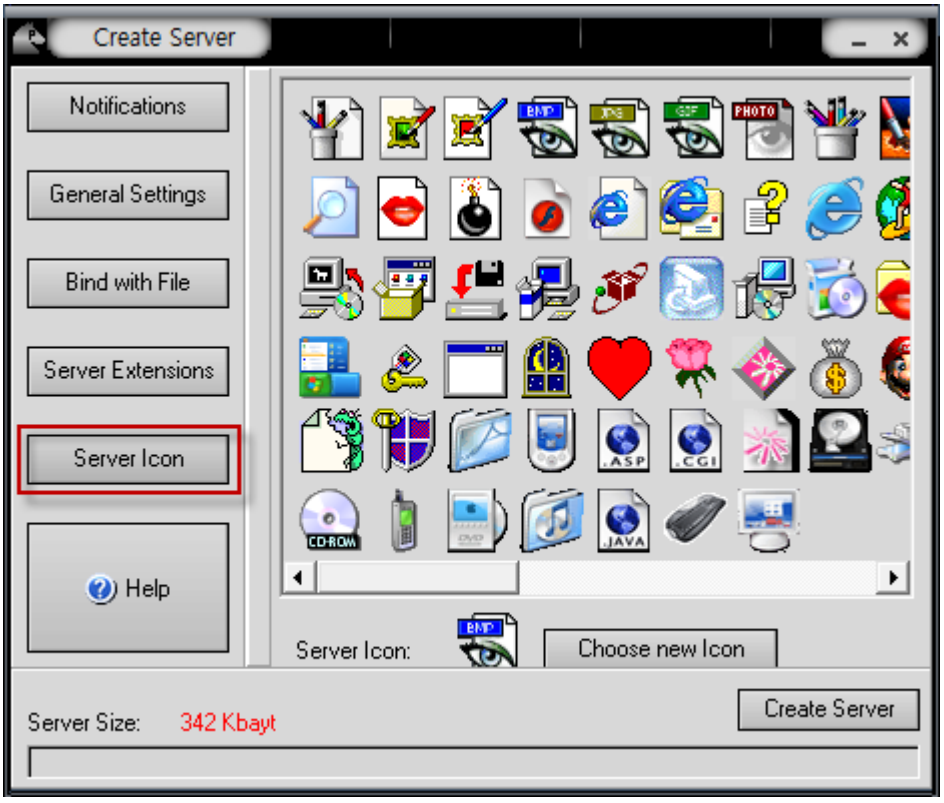
그 밑에 4가지 옵션은 필히 체크를 해야될것들인데 다들 윈도우에서의 서버 파일실행상태를 감추기 위한 기능들.



서버파일하고 함께 묶을 파일을 선택.

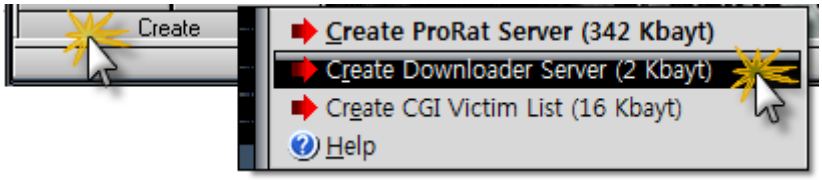

Create Server
Notifications
General Settings
Bind with File
Server Extensions
Server Icon
Help
Select Server Extension
EXE (Has icon support)
SCR (Has icon support)
PIF (Has no icon support)
COM (Has no icon support)
BAT (Has no icon support)
Server Size:
342 Kbayt
Create Server

서버파일 확장자 선택.



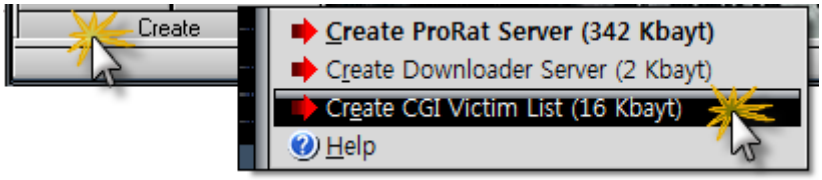
서버파일 icon 선택.

설정이 끝났으면 "Create Server"을 클릭하여 파일 생성.



만약 다운로드서버를 생성하고 싶다면 두번째 메뉴를 선택. 제가 실행을 하니 에러가 뜨더라구요. 윈도우7 이라 그런가? 기회가 되시는분들은 윈도우xp

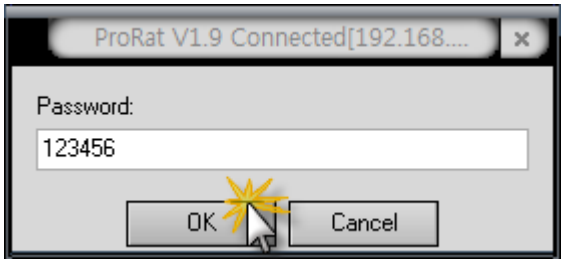
에서 한번 실행을 해보시길.



웹사이트로 좀비피씨의 접속정보를 확인하고 싶다면 3번째 메뉴를 클릭하여 CGI파일을 만들어야 되겠죠. 실행을 하시면 아래와 같은 창이 뜰거구요.

(0) 은 웹페이지에 접속시 필요한 패스워드. (1)은 cgi파일명. (2)는 데이터를 저장할파일. 즉 좀비pc정보들. (3)은 한페이지에 보여질 좀비PC수. 설정이 끝났다면 "Create CGI files"를 클릭하면 Prorat폴더내에 cgi-bin 폴더가 생성될건데요. 안에 보시면 파일두개가 있는데 그걸 cgi실행을 지원하는 웹호스팅계정에 업로드하시면 끝. 물론 데이터저장파일 권한은 777로.

서버파일을 생성하였다면 감염시킬 컴퓨터에 실행시키고(여러가지 방법이 있겠죠? ^^) 좀비PC 아이피를 입력하고 포트를 설정하고 "Connect"를 클릭하면 패스워드 입력창이 뜰거구요. 설정한 패스워드를 입력하고 "OK"를 클릭.

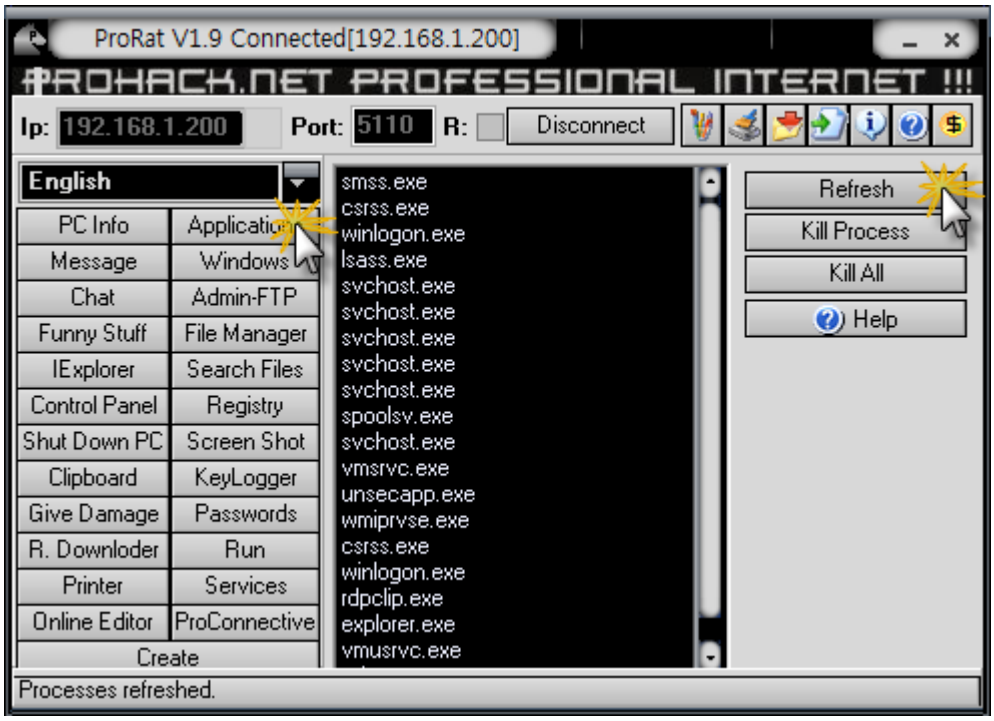


정상적으로 접속이 되었다면 아래와같이 "Password coreect..." 패스워드가 정확하다는 메시지와 함께 접속완료.

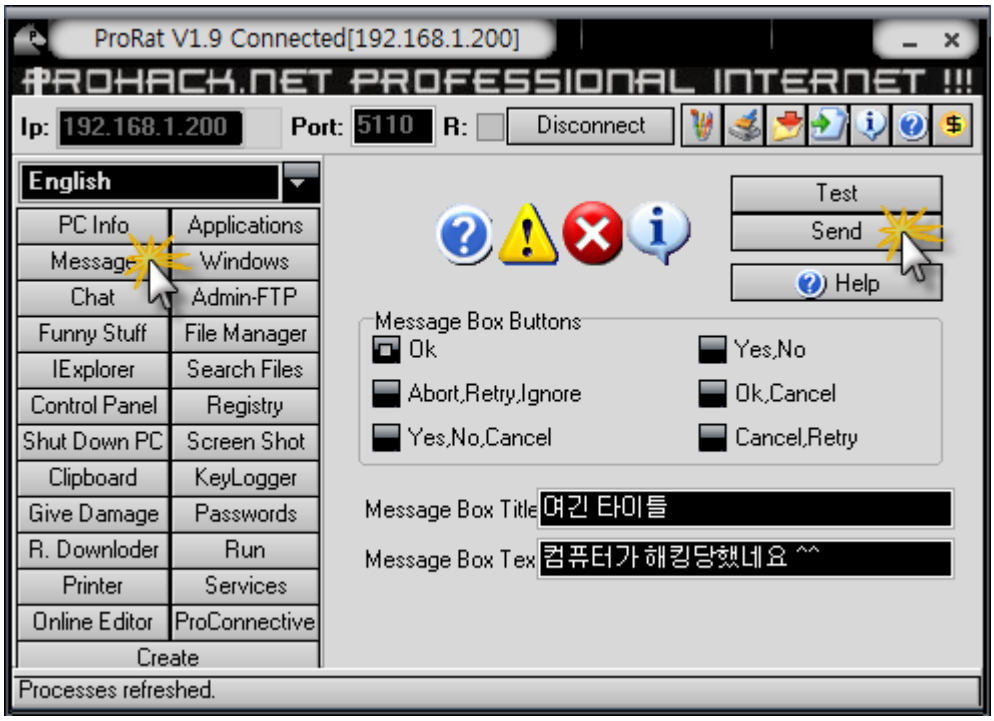
그리고 접속이 정상적으로 되었다면 위와같이 "Connect" 버튼이 "disconnect" (접속끊기) 버튼으로 바뀌어지는 것을 확인가능.

왼쪽 메뉴리스트 맨위를 보시면 인터페이스 언어를 선택할 수 있는 기능이 있는데요 아직은 한국어는 없구요. (현재 한글로 해석중). 영어를 선택합니다.

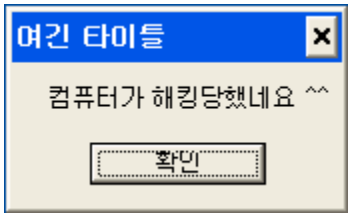
"PC info" 버튼을 클릭하면 좀비피씨의 각종정보를 확인가능.

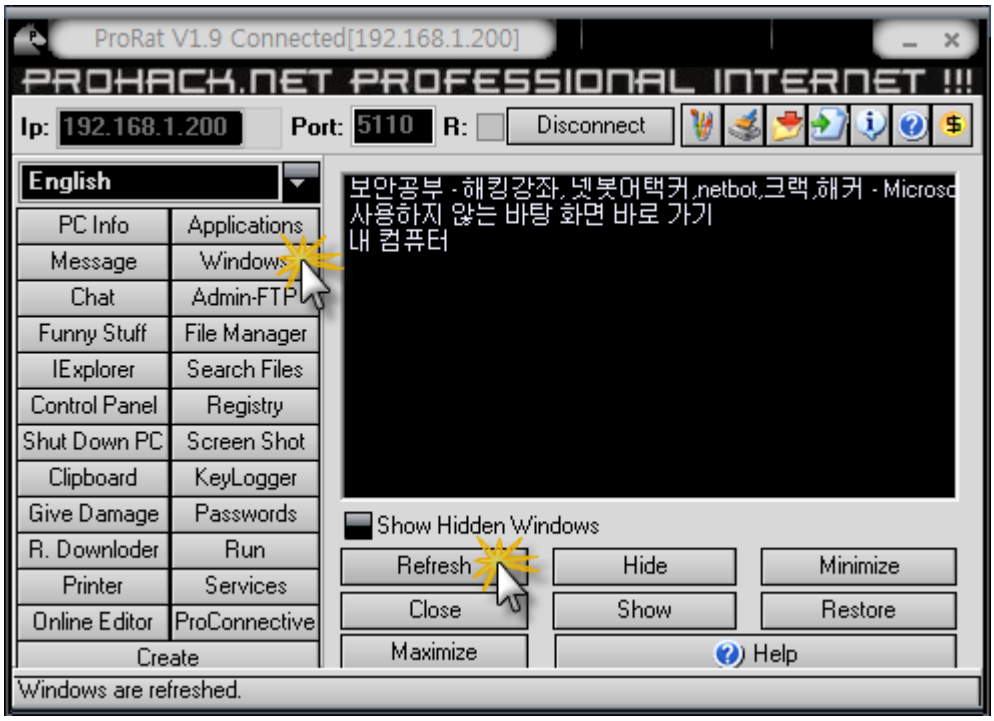


"Applications" 버튼을 클릭하고 "Refresh" 를 클릭하면 현재 실행되고있는 프로그램들의 프로세스를 확인가능. 만약 특정 프로세스를 Kill 하고 싶다면 선택하고 "kill process" 버튼을 클릭하면 되구요. "Kill All"버튼은 킬올. ^^;;

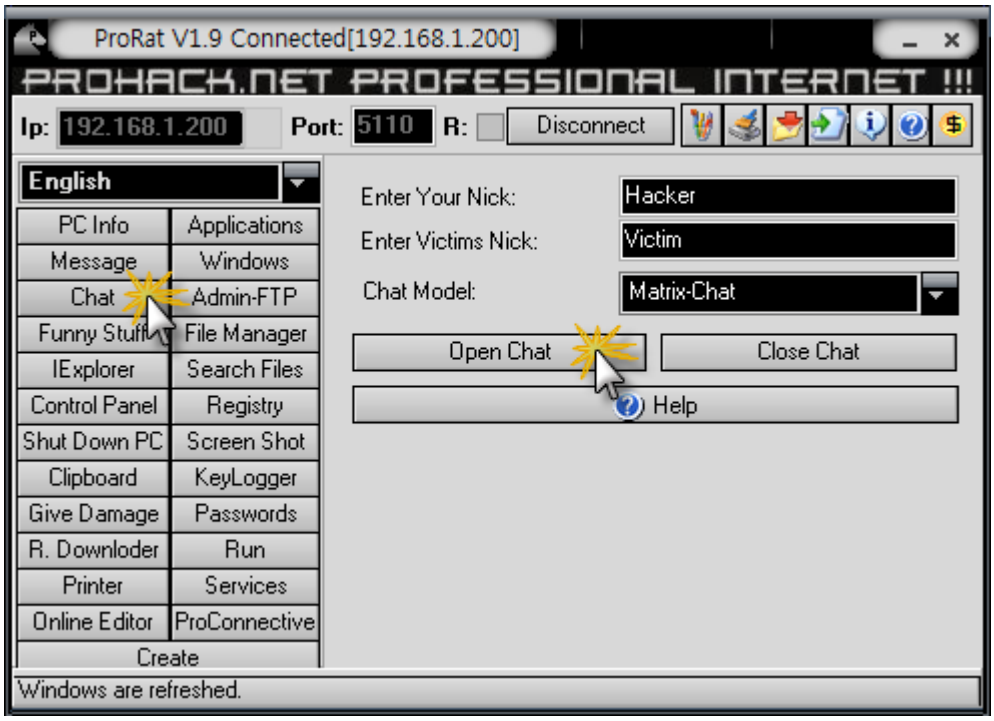


"Message"버튼은 현재 제어하고있는 좀비피씨에 에러창을 띄우는 기능이구요. 에러창 형태와 보여질 메시지를 위와같이 입력하고 "Send"버튼을 클릭하면 좀비피씨에는 아래와 같은 윈도우 창이 뜨죠. ^^

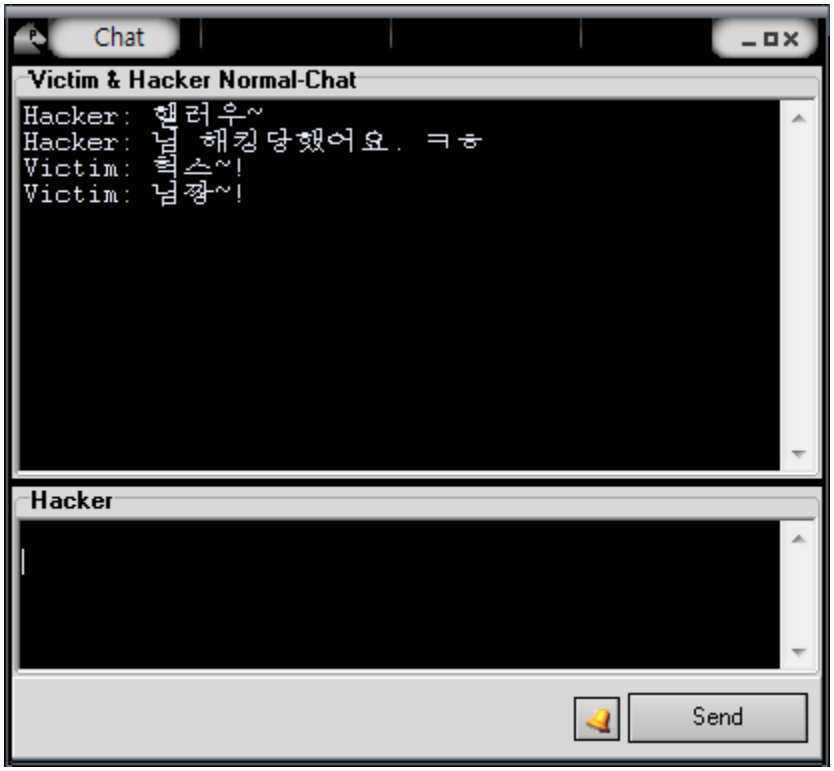




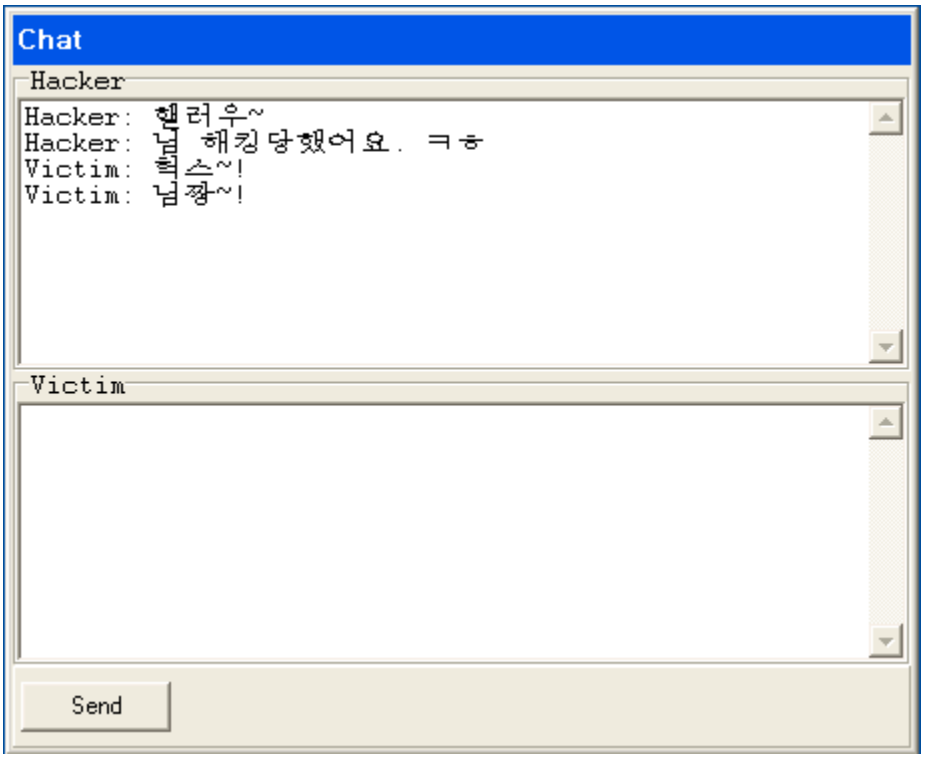
"Windows"버튼을 클릭하고 "Refresh"버튼을 클릭하면 현재 좀비PC에 실행된 윈도우창들의 이름을 확인가능. "Hide"는 감추기. "Minimize"는 최소화등 기능을 확인하실수있습니다.



"Chat"는 말그대로 채팅기능. "Open Chat"를 실행하면 채팅창이 뜰거구요 좀 비PC사용자와 채팅을 즐길수있음. ^^; 아래는 해커의 채팅장.

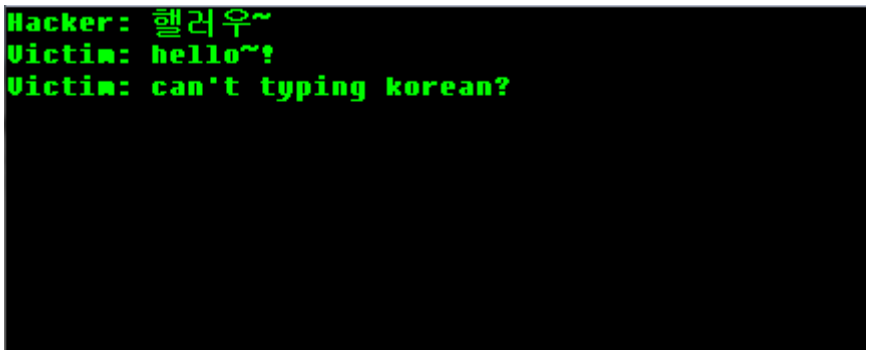


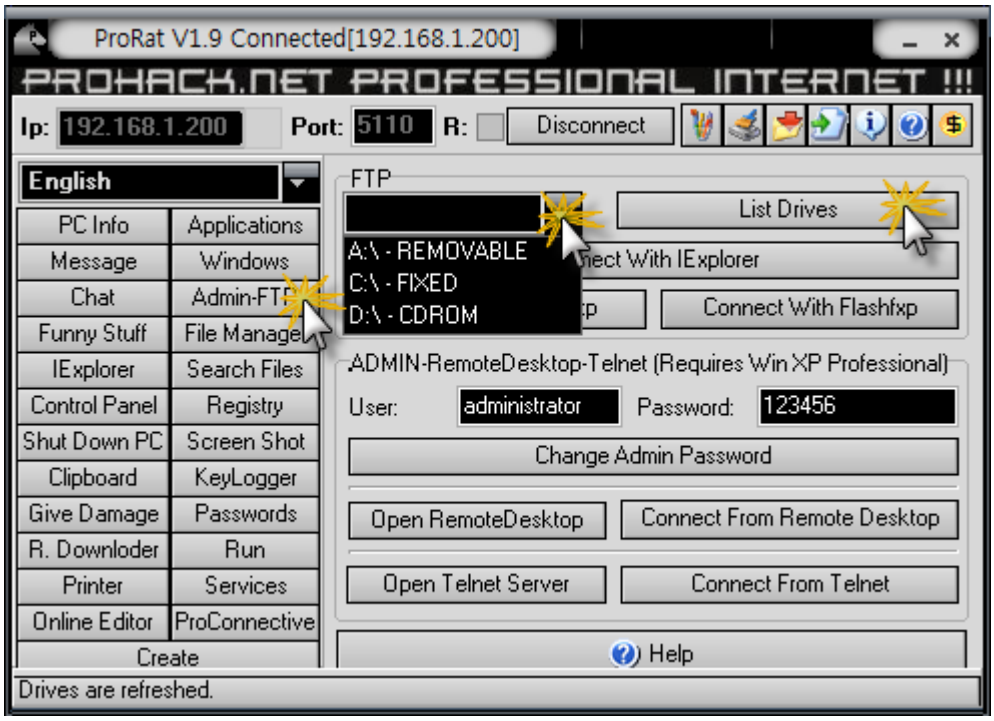
아래는 좀비PC의 채팅창.



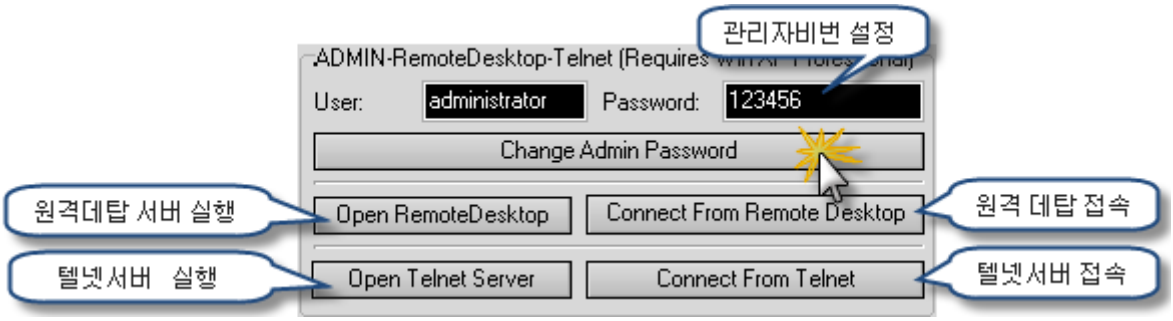
채팅기능을 실행시 만약 매트릭스모드를 선택하셨다면 아래와같이 전체화면이 검은색바탕으로 변할거구요. 매트릭스에 나오는 주인공처럼 채팅가능.

하지만 좀비PC에서는 한글지원이 안된다는...



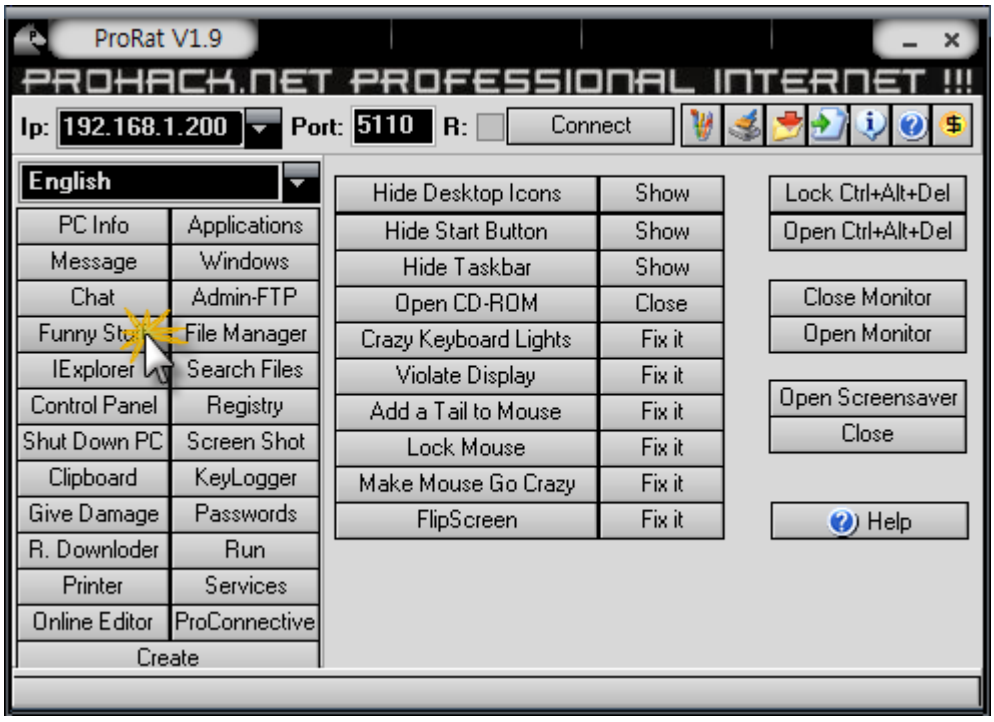


"Admin-FTP" 기능은 말그대로 FTP로 파일을 전송하는 기능. "List Drives"를 클릭하면 현재 좀비피씨의 드라이브가 보여질거고 그중에 파일을 다운받고 싶은 드라이브를 선택하고 IE로 혹은 cuteftp, Flashfxp 같은 ftp클라이언트로 파일을 다운받을수있음.

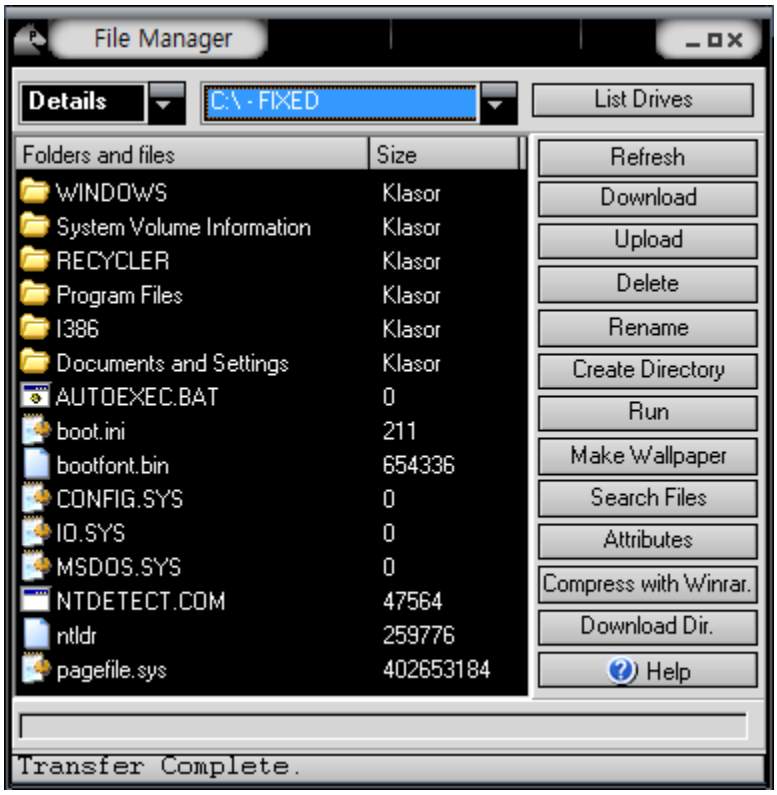


아래는 관리자 패스워드를 설정하는곳인데 아쉬운 것은 사용자를 추가하거추 하는 것이 아닌 관리자 비번을 수정하는것이라 쉽게 발견된다는 것이 좀 그렇네요. 그 아래는 데탑서버실행하고 접속하는 기능과, 텔넷서버를 실행하

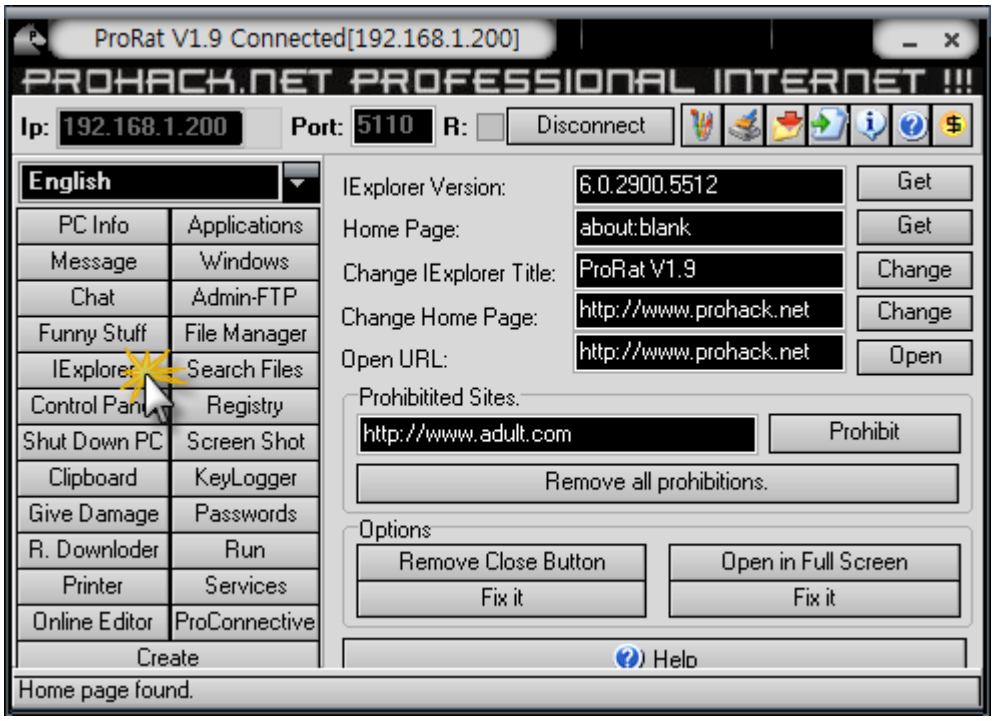
고 접속하는 기능.



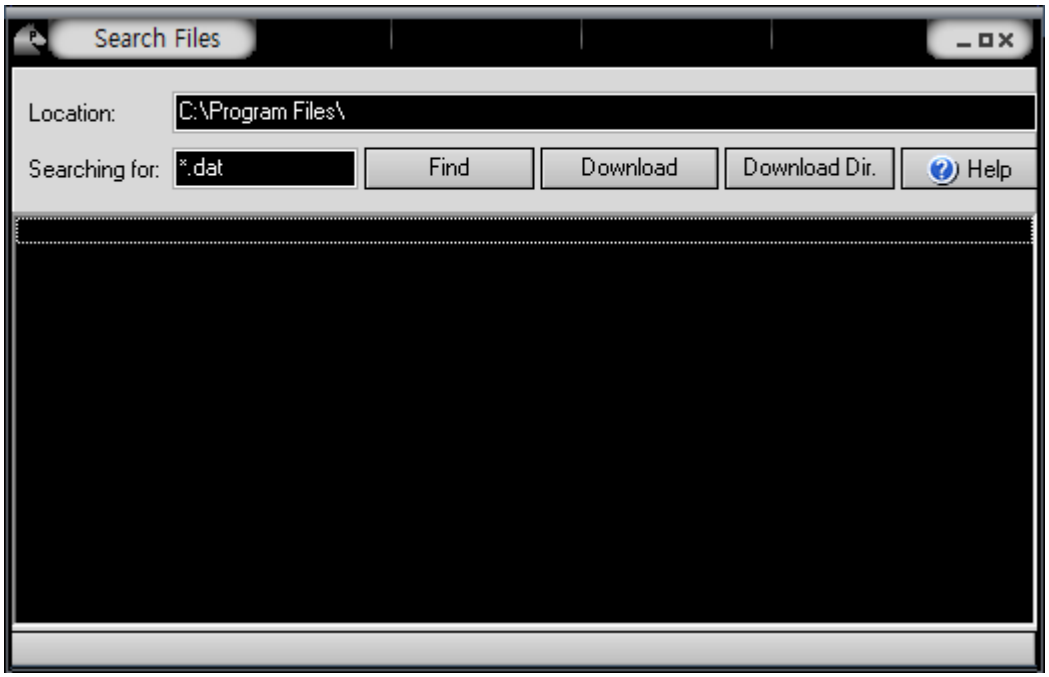
"Funny Stuff" 는 말그대로 잼있는 기능들을 모아둔 기능페이지. 쉽게 알아볼 수있는 기능들이라 설명은 줄이도록 하겠습니다~ ^^



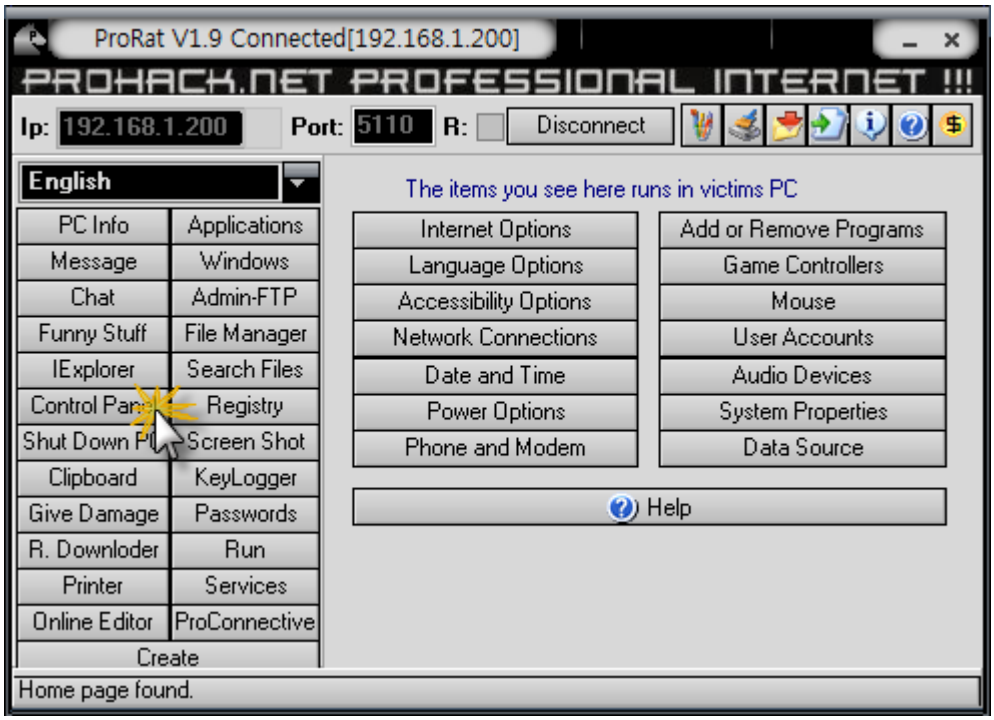
다음은 "File Manager" 기능. 그냥 그대로 파일매니저기능. ㅋㅎ 기능도 전에 쓴 넷데빌 사용법하고 동일.



"Iexplorer" 는 IE브라우저 정보를 가져오고 수정하는 기능. "Iexplorer version" 는 IE버전 가져오기 "home page"는 설정된 홈페이지정보 가져오기. "change iexplorer title"는 ie브라우저 타이틀수정. "change home page"는 홈페이지 수정하기. Prohibit는 접속불가능하게할 사이트를 입력하고 "prohibit"버튼을 클릭하면 좀비pc는 해당사이트에 접속불가. "remove close button"는 (x)창닫기 버튼을 감추기. "Fixt it"는 되돌려놓기 . "Open in full screen"은 전체창모드로 만들기와 "fix it"는 되돌려놓기.

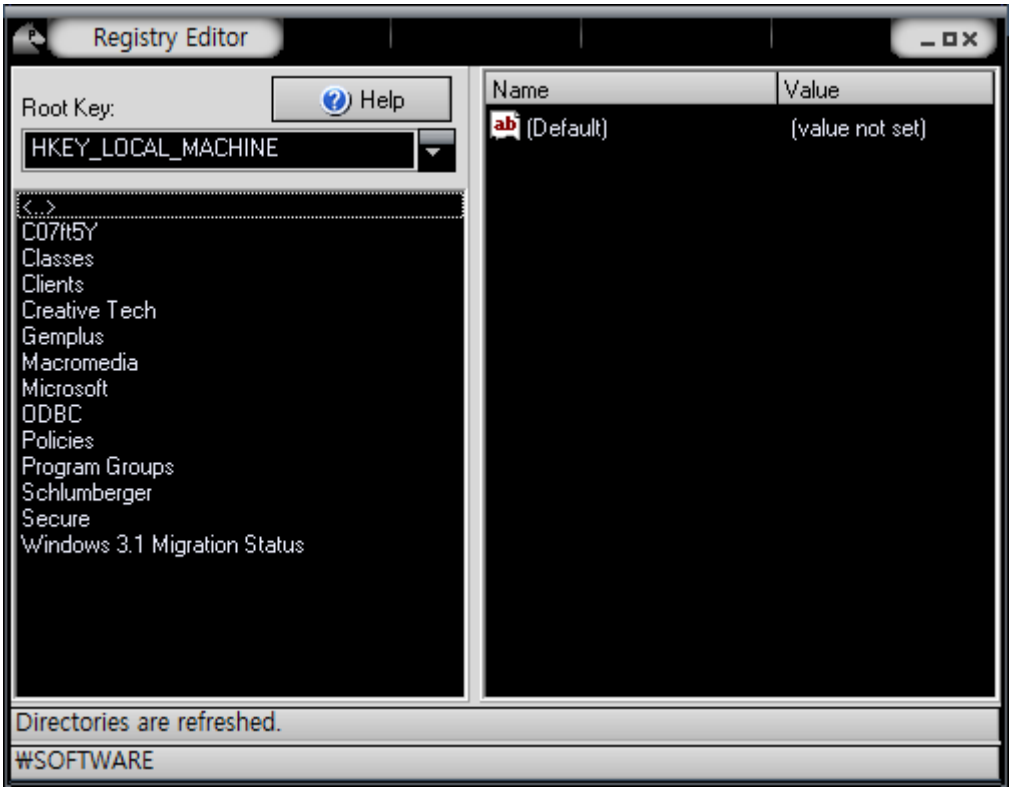


"Search files"는 파일검색 기능.

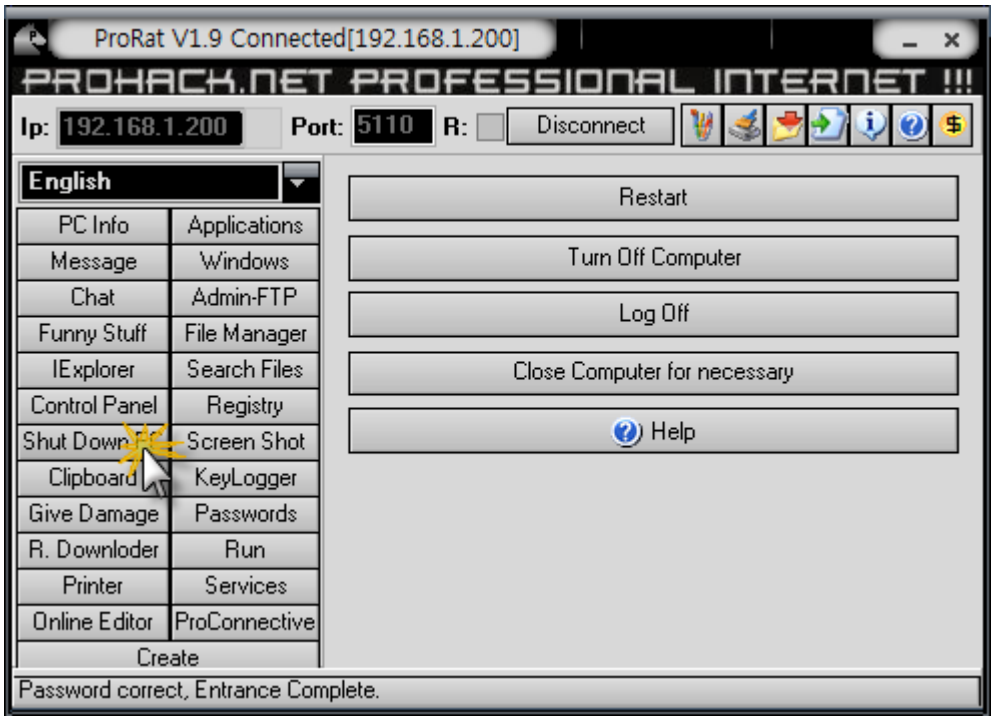


"control panel"은 "제어판"의 각종 기능을 실행하는 기능. 예를 들면 언어설

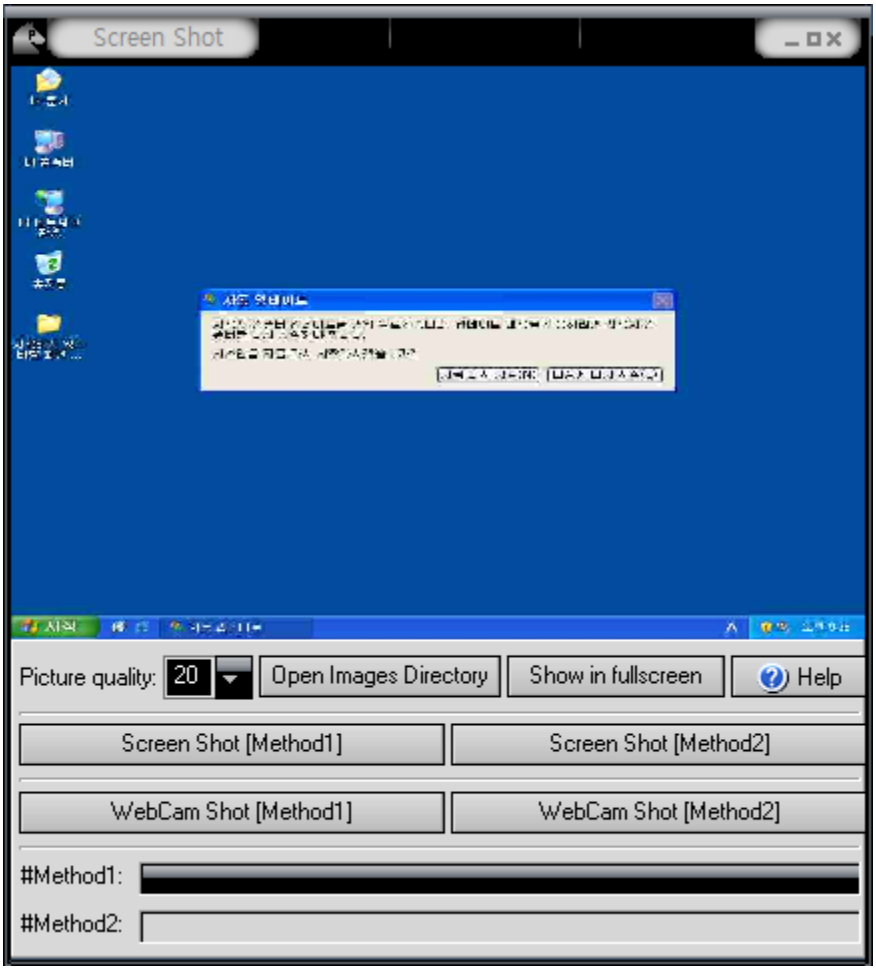
정, 혹은 파워설정.



"Registry Editor" 은 로컬에서 레지스트리 편집기를 사용하는것과 동일하구요.



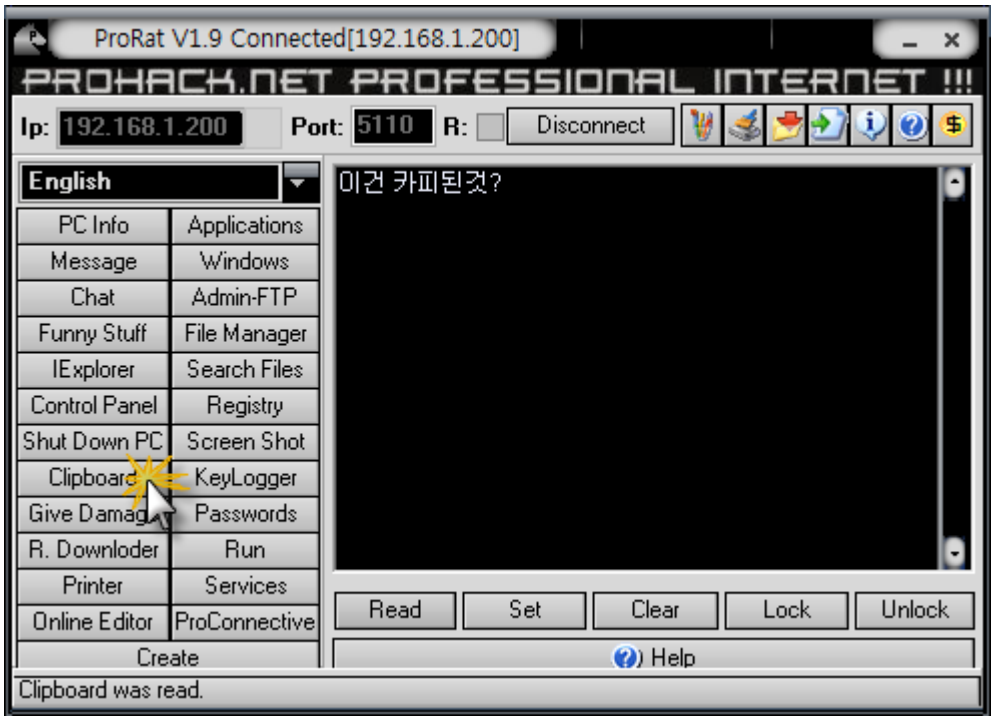
"Shut down PC"는 컴퓨터를 "재부팅", "끄기", "로그오프" 등 기능들을 수행할 수있는 기능.



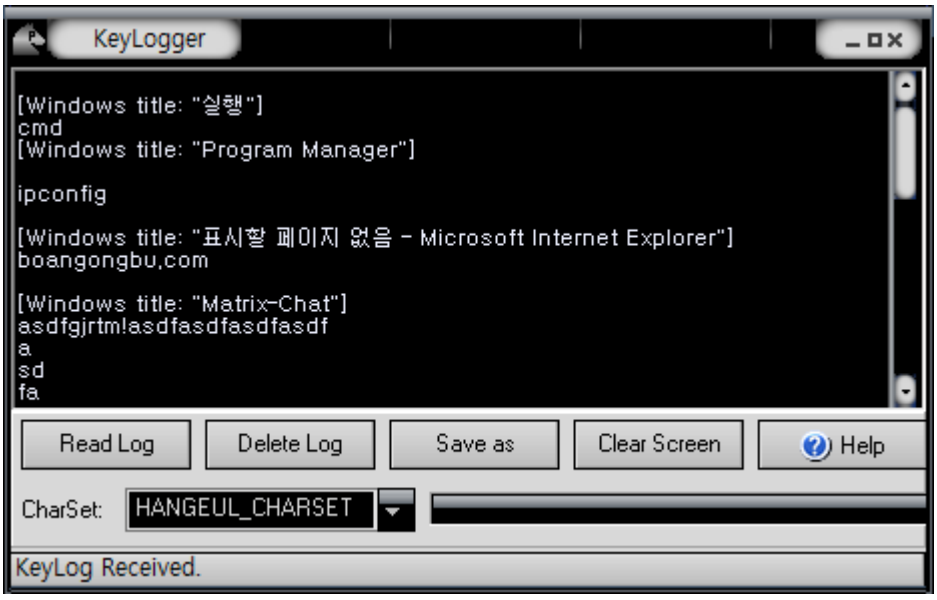
음... "Screent shot"... 스크린샷 기능. 역시 이런기능이 잼있겠죠? ㅎㅎㅎ

화질선택이 가능하구요. 전체창으로 감시가능. 그리고 바탕화면뿐만 아니라.

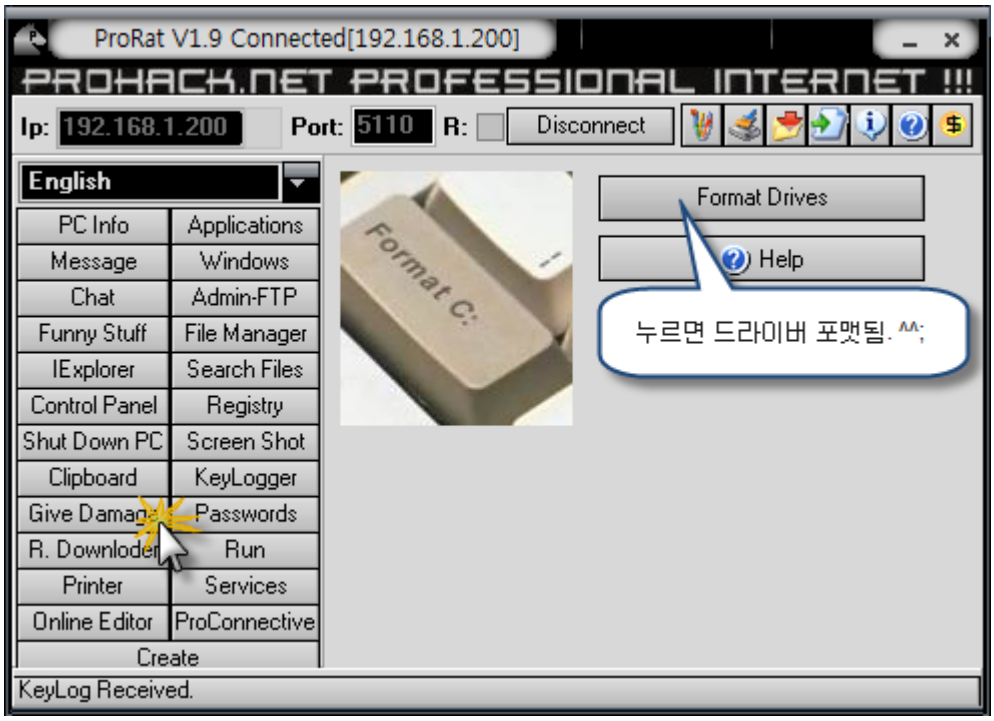
만약 좀피pc에 웹캠이 설치되어있다면 웹캠도 감시가 가능하구요.



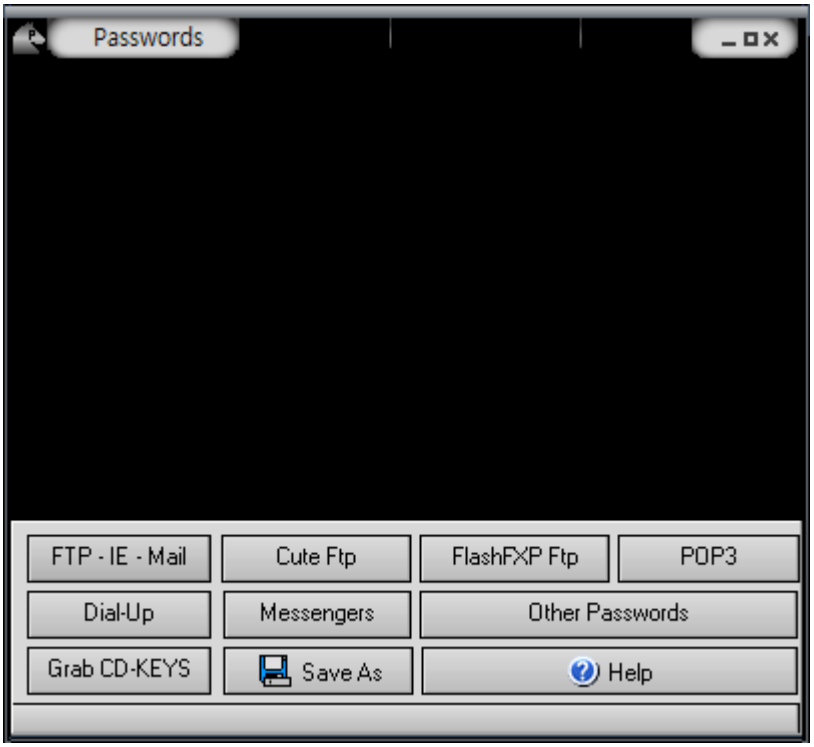
"Clipboard" ... 현재 클립보드에 저장되어있는 내용을 확인가능.



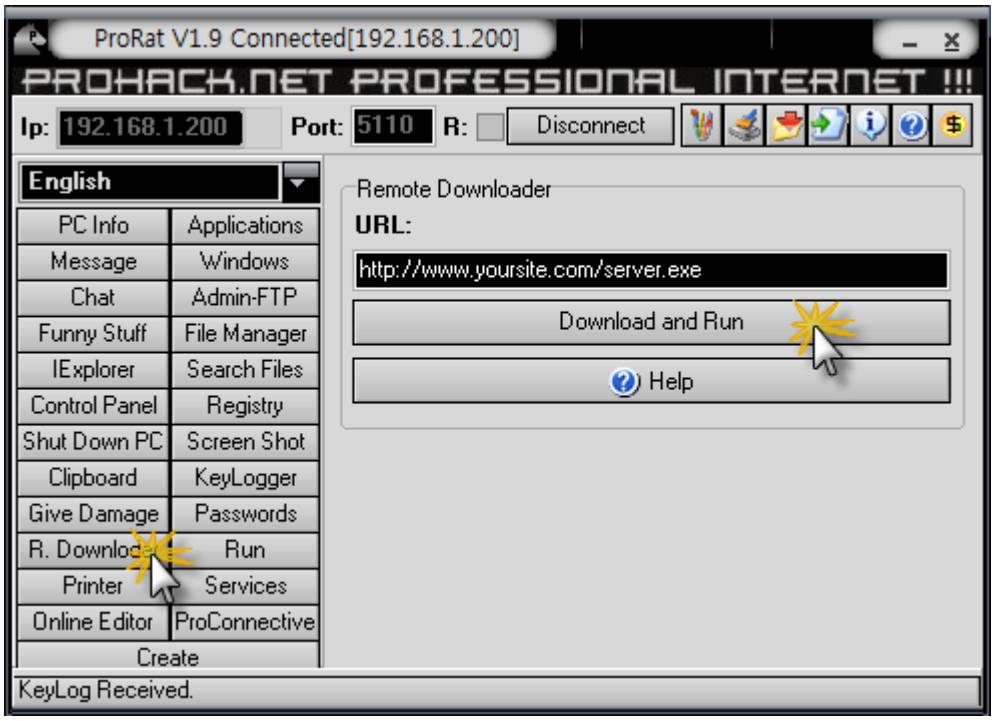
"key Logger" 트로잔이라면 빠져서는 안될 키로거 기능. "Read log"를 클릭하면 저장된 로그들을 확인가능.



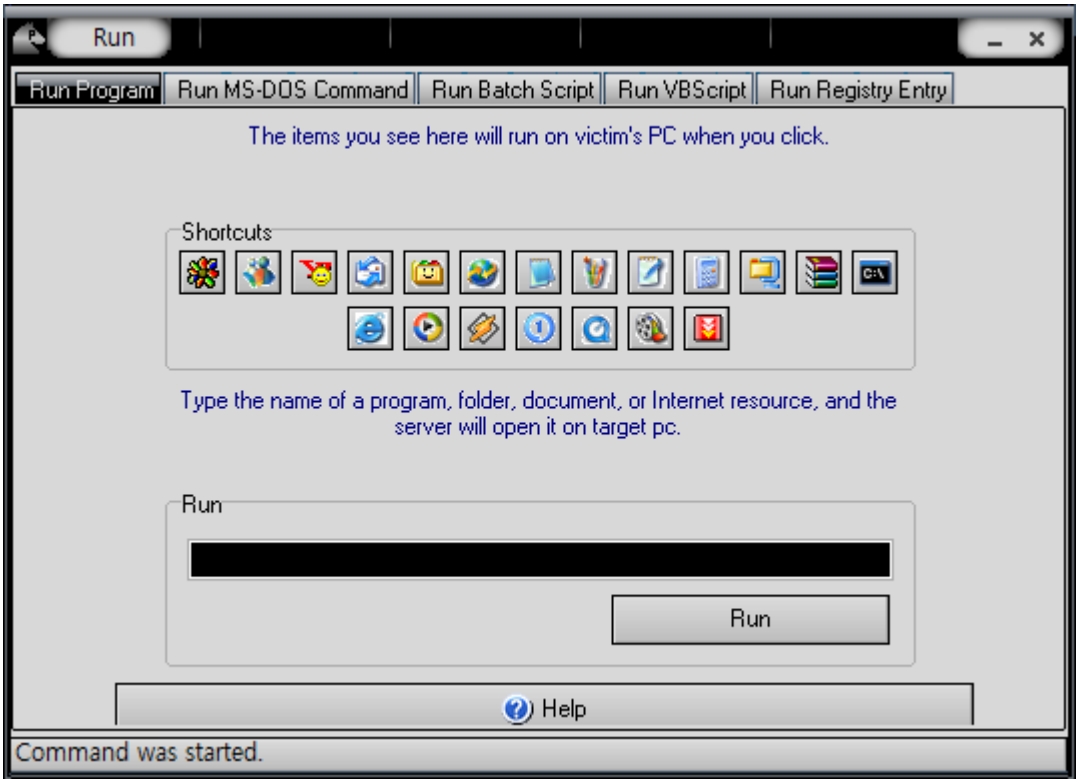
"give damag" 처음에는 데미지를 준다구해서 PC를 다운시키는 기능인줄로 알았는데. 드라이브를 포맷시키는 기능... 덜덜...;;;



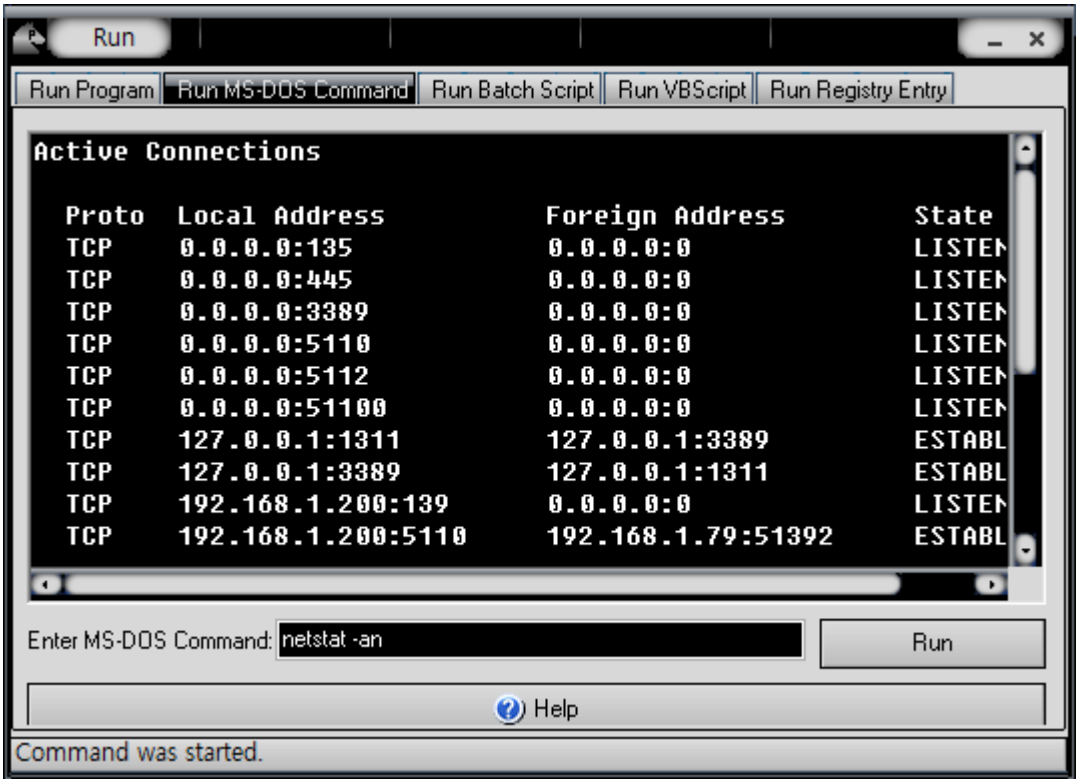
만약 좀비PC에 웹사이트 패스워드가 저장되어있거나. Cuteftp, flashfxp ftp, pop3, 전화접속등 패스워드가 저장되어있다면 클릭한번으로 이 패스워드들을 확인가능.



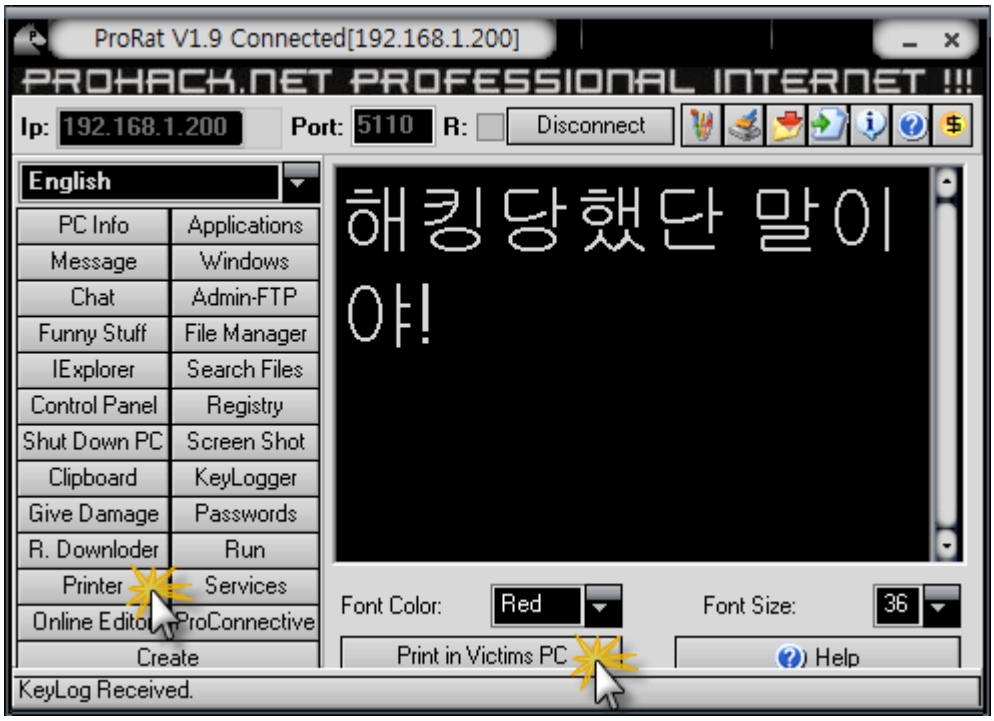
"R.download" 특정 웹사이트 파일을 좀비피씨에 다운로드 받는 기능.



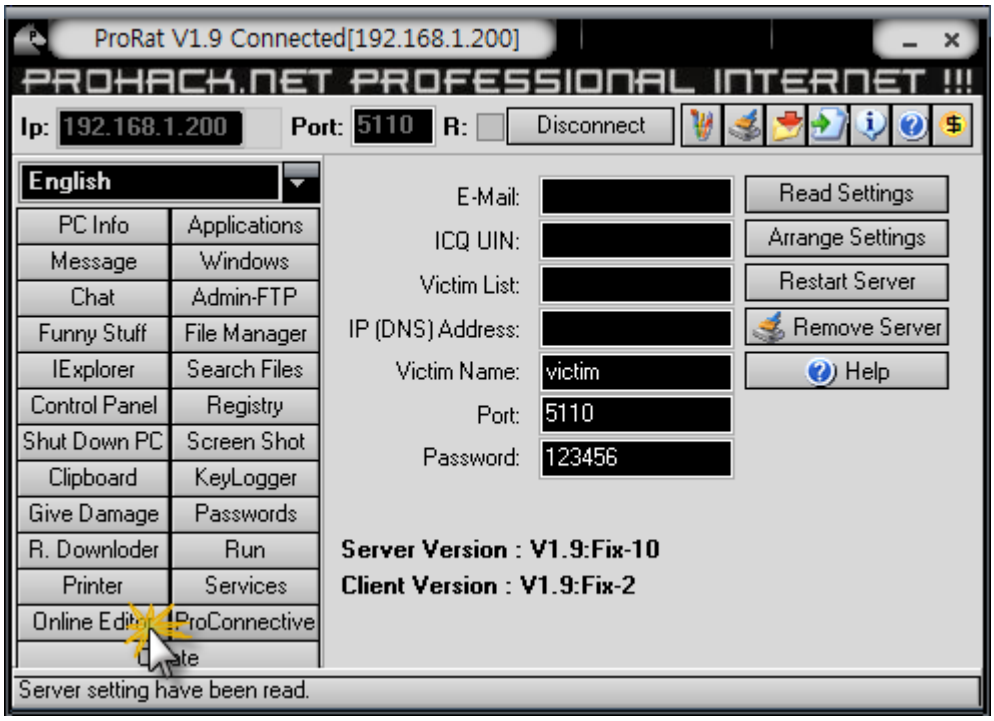
위는"Run" 기능인데요. 좀비pc에서 실행시킬 프로그램을 클릭하거나 입력하여 실행시킴. 위에 탭을 선택하여 명령어를 실행하거나 Batch 스크립트를 편집하여 실행하거나, vbscript를 실행하거나 레지스트리 파일을 실행시킬수있음. 아래는 명령어를 실행시킨 화면.



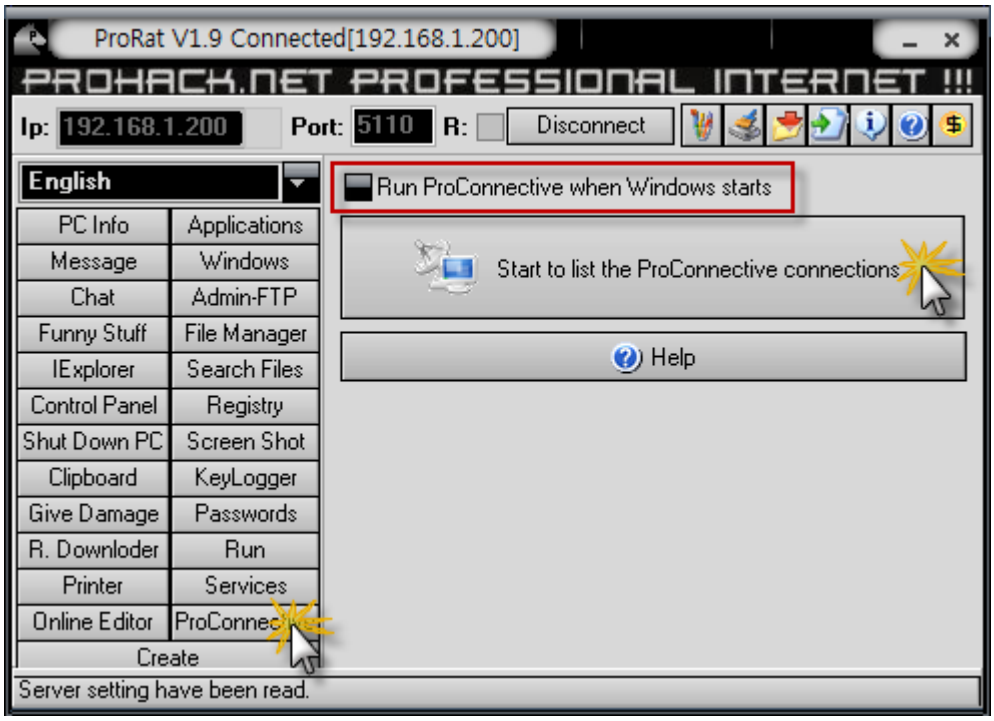
아래는 "Printer"기능인데요. 좀비pc에 프린터가 연결되어있고 전원이 켜져있다면 여기에 프린트하고싶은 내용을 입력하여 "Print in victims pc" 를 클릭하면 그대로 프린트 됨. ^^



그다음은 "Services Manager" 기능. 윈도우서비스들을 관리하는 기능. 윈도우 자체의 그것과 동일.



"Online Editor"기능은 현재 제어하고있는 좀비PC의 접속알림 이나, 접속포트, 혹은 패스워드를 수정할 수 있는 기능이구요. 현재 설정된 정보를 확인하려면 "Read Settings"를 클릭하면 되구요



"Start to list the Proconnective connections". 여기서 말하는 "Proconnective"는 전에 서버파일을 생성시 사용된 리버스컨넥션을 말하는거구요. 커다란 저 버튼을 클릭하면 현재 온라인된 모든 감염된 pc를 확인가능. 만약 좀비PC가 내부네트웍에 위치하여있다면 유료 프로그램을 사용하는 사용자만 제어가 가능하구요 일반 무료프로그램 Public 버전을 사용하는 사용자는 좀비PC가 다이렉트로 인터넷에 접속을 하여야만 이 기능을 제어가 가능하게 설계되었군요. 그리고 주의해야될 것은 만약 제어자 즉 해커의 컴퓨터가 내부망에 있다면 라우터에서 4110, 4112, 5110, 5112, 41100, 51100 이 포트들을 해커의 컴퓨터에 매핑되게 설정하여야 제어가 가능하구요.